DEPARTMENT OF VETERANS AFFAIRS
VETERANS HEALTH ADMINISTRATION
VISN 7 VA SOUTHEAST NETWORK

Memorandum 10N7-118
January 2008

REMOTE ACCESS SECURITY

1. PURPOSE: To establish expectations and responsibilities in providing remote access connections, from government furnished equipment (GFE) and non-VA owned equipment, to the VA network and in securing these connections from compromise.

2. POLICY:

a. Remote users are required to connect to the VA network utilizing the national One-VA VPN solution. A generic dialup Internet Service Provider (ISP) is provided with the One-VA VPN solution if the remote user does not have an Internet service provider at home or at the alternate remote location.

b. Each medical center will document, monitor, and control remote access to the information systems, including remote access for privileged functions.

c. VA employees, contractors, subcontractors, and volunteers may transport, transmit, access, and use VA sensitive information outside of VA facilities ONLY WHEN their VA supervisor and Medical Center Director authorizes such action in writing. ALL SENSITIVE INFORMATION APPROVED TO BE TRANSPORTED MUST BE ENCRYPTED USING VA APPROVED, FIPS 140-2 CERTIFIED PRODUCT.

d. Use of or access to VA sensitive information may be revoked, modified, or limited at any time by the user's VA supervisor, the Medical Center Director, or the facility CIO (FCIO).

e. All memoranda of understanding, contracts, statements of work, IRBs, and data use agreements will include assertions that all parties will conform to these remote use policies and procedures.

f. Users will not simultaneously connect to VA and one or more non-VA networks (also known as split tunneling).

g. Only VA personnel may access VA-owned equipment used to process VA information or access VA processing services. Users may not share with non-VA employees or unauthorized personnel instructions or information regarding how to establish connections with VA private networks and computers. Users may not share remote access logon IDs, passwords, and other authentication means used specifically to protect VA information or access techniques to VA private networks.

h. Remote access is allowed and controlled through the National One VA VPN. The National One VA VPN controls all remote accesses through a managed access control point. All requests for One VA VPN accounts must be approved by the immediate supervisor, the FCIO, and the facility Information Security Officer (FCIO). The National

One VA VPN uses a "time-out" function that requires re-authentication after 30 minutes of inactivity.

i. In regonition of its responsibility to secure and safeguard information from misuse or improper disclosure, all remote access service computer users must provide proper justification of the need for access, and sign the Department of Veterans Affair (VA) National Rules of Behavior prior to remote access being granted. Approved remote access users can access VA systems from their residence or while they are on travel status using furnished GFE (Government Furnished Equipment). If non-VA owned equipment must be used in certain circumstances, a waiver must be in place. All of the security controls required for GFE must be utilized in approved non-VA owned equipment and must be funded by the owner of the equipment. Approved remote access users are governed under the same local policies, federal laws and regulations that apply to all local users of VA computer systems and the security and privacy of the information contained therein.

j. Responsibility for access to, or training on systems not covered by this policy lies soley with the individual or service/section requiring this access. Remote access to VA computer systems does not constitute approval of overtime pay or compensatory time.

3. ACTION(S):

a. Users are responsible for requesting remote access through their supervisor. Users must complete Attachment A, Remote Access Request and Remote Computing Security Agreement, must have completed the mandatory Privacy and Information Security Awareness Training, and provide a signed Department of Veterans Affairs (VA) National Rules of Behavior. All requests must be forwarded to the ISO through the applicant's supervisor or Service Line Manager. The application should include a justification for remote access with concurrence by the supervisor or Service Line Manager. Once the application is approved the user will be issued GFE to be used to connect remotely. The user is responsible for returning the equipment to be inventoried and updated according to the local facility inventory policy. This will be at least every 90 days or less. If there are certain circumstances in which GFE cannot be issued for remote access a waiver must be submitted to the FISO and FCIO. Once the waiver is submitted the user will be provided the installation software necessary to install One-VA VPN, HIPS RealSecure firewall, and McAfee VirusScan (if necessary). The remote user must ensure that the remote workstation complies with the following requirements to secure their computer:

- For personally-owned computers, the remote users must ensure that the latest virus definition files for the anti-virus product installed on their computers is routinely updated at least once per week.

  In addition, a current hardware or software firewall product must be installed if the personally-owned computer is used for official VA business. RealSecure software is available free of charge via the VA Enterprise-wide licensing agreement from the One-VA VPN installation disk to home users if their personally-owned computer is used to conduct VA business, or they may use any other third party software or hardware firewall product, provided that the product is routinely updated.

- All remote access workstations are required to complete all 'Critical Updates' located at http://windowsupdate.microsoft.com weekly or immediately upon logging into the VA network if more than a week has passed since the last update. This is applicable for all versions of the Windows operating systems.
- If the user has more than one personally-owned computer attached through a home network, all computers on the home network must comply with the above virus, firewall, and patching requirements.

If it is determined that a user is violating this policy remote access privilege will be revoked. The remote user must complete the security procedures and sign another Rules of Behavior before remote access is granted. If the user continues to violate compliance with this policy remote access will be deactivated and not reissued. Continuos violations will be reported to the user's supervisor to determine if disciplinary action should be taken.

b. Contractors and non-VA employees may submit requests for access in writing to the FISO and FCIO through the COTR or agency sponsor. Each identified contractor or non-VA employee must complete and sign Attachment A, Remote Access Request and Remote Computing Security Agreement, must have completed the mandatory Privacy and Information Security Awareness Training, and provide a signed Department of Veterans Affairs (VA) National Rules of Behavior. All contractors and non-VA employees are required to follow the same policy and procedures and will have the concurrence of a higher level official within the facility or network. Codes will be delivered to the contractor either electronically using PKI or in a sealed envelope to the FISO, FCIO, COTR or agency sponsor for distribution to the approved user. Vendors and affiliates may have a Site-to-Site VPN connection to VA's network. Requirements for access for a Site-to-Site VPN connection are not covered by this policy. Contact the facility ISO for procedures to request a Site-to-Site VPN.

4. RESPONSIBILITIES:

a. The FCIO is ultimately responsible for the implementation and compliance with this policy. The FCIO is also responsible for developing a process for issuing GFE to VA employees approved for remote access. When GFE is not available or other circumstances prevent the use of GFE the FCIO will coordinate the waiver process. The FCIO is responsible for communicating this policy and providing training on the remote access software and hardware.

b. The FISO is responsible for administration and control of this policy for all VA staff, contractors, and business partners. The ISO will maintain an electronic or paper record of all requests for VPN access. Records should be readily available for higher review.

c. The One VA VPN web portal provides a listing of all active VPN accounts for quarterly review by the ISO. The One VA VPN Administrator will disable any VPN account that has been inactive after 90 days, and will delete any VPN account that has been inactive for more than 180 days. The VPN user can contact their ISO or the One VA VPN Help Desk to enable a disabled account. Users whose accounts have been deleted must go through the One VA VPN application process.

d. Service Line Managers and supervisors are responsible for reviewing all requests for One-VA VPN access and ensuring reasonable justification is provided. Supervisors are responsible for contacting the FISO and FCIO to ensure remote access privileges are terminated as soon as they are no longer needed, when the account owner transfers, retires, resigns, or is terminated. Upon termination of access the supervisor will recover and return any issued GFE to the EIL owner.

e. The One VA VPN Helpdesk is responsible for providing technical support for One-VA VPN installations and can be contacted at .

f. All VA staff, contractors, and business partners are responsible for complying with VA remote access security measures as documented in "VA Remote Access Guidelines".

5. REFERENCES: VA Directive and Handbook 6500, Information Security Program.

6. RESCISSIONS: None

7. RECERTIFICATION: This VISN 7 Memorandum is scheduled for recertification on/or before the last working day of February 2010

Lawrence A. Biro
VA Southeast Network, VISN 7

Distribution:
Medical Centers Directors (00), VISN 7
Facility IS Officers, VISN 7

Department of Veteran Affairs – Attachment A
VISN7 One-VA VPN Remote Access Request Form and Security Agreement

1) LAST NAME	2) FIRST NAME	3) MIDDLE INITIAL	4) NICKNAME

5) SERVICE LINE or CONTRACTOR COMPANY	6) DATE OF BIRTH	7) MAIL CODE OR ADDRESS	8) PHONE/EXT

9) POSITION TITLE	10) Last 4 SSN	11) DUTY LOCATION (Campus, Bldg, Room)
	_____	

12) <u>Operating System (right-click ONCE on the "My Computer" desktop icon, then "Properties" to determine O/S):</u>

- ☐ Windows 2000
- ☐ Windows NT
- ☐ Windows 95/98/98SE/Millenium Edition
- ☐ Windows XP Home/XP Professional
- ☐ Other O/S:

_____

13) NT Username (vha*xxxxxxxx*):

_____

VA e-mail address (*name*@va.gov):

_____

_

14) For the PC which will be used to remotely connect to the VHA computer network, please check all that apply:

- ☐ **1. VA-Owned PC has McAfee anti-virus software installed**

– or –

- ☐ **Personally-owned PC has other anti-virus software installed. Specify publisher: _____**
- ☐ **PC has latest definition (DAT) file installed.**
- ☐ **1.) VA-Owned PC has HIPS RealSecure software firewall product installed.**

– or –

- ☐ **2.) Personally-owned PC has a other firewall installed/connected. Specify manufacturer:_____**
- ☐ **PC has all "critical updates" applied from the Windows Update website.**

– or –

- ☐ **PC is not a Windows machine, but has current anti-virus, firewall, and O/S updates installed.**

Remote access will NOT be granted until all items above have been installed. By signing below, you agree to update your virus software with the latest DAT files and update your operating system with the latest Windows Update "critical updates", both on a weekly basis.

22) Requestor's Signature attesting to protection requirements above:	**23) Print Name**	**24) Date of Request**

25) Notice: Remote users will comply with VISN 7 and national Information Technology policies while connected to any VA IT resources remotely. Remote users will take appropriate measures to safeguard the VA IT resources from unauthorized access and malicious activity. The VA accepts no responsibility for personally owned computers, peripherals and/or software.

26) Justification for remote access to VA information resources:

26) Approving Svc Mgr Printed Name (required):	**27) Approving Svc Mgr Signature/Date (required):**	**28) Telephone/Ext:**

29) Approving ISO Signature:	**30) ISO Station Assignment:**	**31) Date of User Security Training**

32) One VA-VPN Software Distribution Date	33) Media Distribution Code	34) ISO Notes:

Department of Veterans Affairs (VA) National Rules of Behavior

I understand, accept, and agree to the following terms and conditions that apply to my access to, and use of, information, including VA sensitive information, or information systems of the U.S. Department of Veterans Affairs.

1. GENERAL RULES OF BEHAVIOR

a. I understand that when I use any Government information system, I have NO expectation of Privacy in VA records that I create or in my activities while accessing or using such information system.

b. I understand that authorized VA personnel may review my conduct or actions concerning VA information and information systems, and take appropriate action. Authorized VA personnel include my supervisory chain of command as well as VA system administrators and Information Security Officers (ISOs). Appropriate action may include monitoring, recording, copying, inspecting, restricting access, blocking, tracking, and disclosing information to authorized Office of Inspector General (OIG), VA, and law enforcement personnel.

c. I understand that the following actions are prohibited: unauthorized access, unauthorized uploading, unauthorized downloading, unauthorized changing, unauthorized circumventing, or unauthorized deleting information on VA systems, modifying VA systems, unauthorized denying or granting access to VA systems, using VA resources for unauthorized use on VA systems, or otherwise misusing VA systems or resources. I also understand that attempting to engage in any of these unauthorized actions is also prohibited.

d. I understand that such unauthorized attempts or acts may result in disciplinary or other adverse action, as well as criminal, civil, and/or administrative penalties. Depending on the severity of the violation, disciplinary or adverse action consequences may include: suspension of access privileges, reprimand, suspension from work, demotion, or removal. Theft, conversion, or unauthorized disposal or destruction of Federal property or information may also result in criminal sanctions.

e. I understand that I have a responsibility to report suspected or identified information security incidents (security and privacy) to my Operating Unit's Information Security Officer (ISO), Privacy Officer (PO), and my supervisor as appropriate.

f. I understand that I have a duty to report information about actual or possible criminal violations involving VA programs, operations, facilities, contracts or information systems to my supervisor, any management official or directly to the OIG, including reporting to the OIG Hotline. I also understand that I have a duty to immediately report to the OIG any possible criminal matters involving felonies, including crimes involving information systems. VA **Handbook 6500 September 18, 2007**

g. I understand that the VA National Rules of Behavior do not and should not be relied upon to create any other right or benefit, substantive or procedural, enforceable by law, by a party to litigation with the United States Government.

h. I understand that the VA National Rules of Behavior do not supersede any local policies that provide higher levels of protection to VA's information or information systems. The VA National Rules of Behavior provide the minimal rules with which individual users must comply.

i. **I understand that if I refuse to sign this VA National Rules of Behavior as required by VA policy, I will be denied access to VA information and information systems. Any refusal to sign the VA National Rules of Behavior may have an adverse impact on my employment with the Department.**

2. SPECIFIC RULES OF BEHAVIOR.

a. I will follow established procedures for requesting access to any VA computer system and for notification to the VA supervisor and the ISO when the access is no longer needed.

b. I will follow established VA information security and privacy policies and procedures.

c. I will use only devices, systems, software, and data which I am authorized to use, including complying with any software licensing or copyright restrictions. This includes downloads of software offered as free trials, shareware or public domain.

d. I will only use my access for authorized and official duties, and to only access data that is needed in the fulfillment of my duties except as provided for in VA Directive 6001, Limited Personal Use of Government Office Equipment Including Information Technology. I also agree that I will not engage in any activities prohibited as stated in section 2c of VA Directive 6001.

e. I will secure VA sensitive information in all areas (at work and remotely) and in any form (e.g. digital, paper etc.), to include mobile media and devices that contain sensitive information, and I will follow the mandate that all VA sensitive information must be in a protected environment at all times or it must be encrypted (using FIPS 140-2 approved encryption). If clarification is needed whether or not an environment is adequately protected, I will follow the guidance of the local Chief Information Officer (CIO).

f. I will properly dispose of VA sensitive information, either in hardcopy, softcopy or electronic format, in accordance with VA policy and procedures.

g. I will not attempt to override, circumvent or disable operational, technical, or management security controls unless expressly directed to do so in writing by authorized VA staff.

h. I will not attempt to alter the security configuration of government equipment unless authorized. This includes operational, technical, or management security controls.
September 18, 2007 VA

i. I will protect my verify codes and passwords from unauthorized use and disclosure and ensure I utilize only passwords that meet the VA minimum requirements for the systems that I am authorized to use and are contained in Appendix F of VA Handbook 6500.

j. I will not store any passwords/verify codes in any type of script file or cache on VA systems.

k. I will ensure that I log off or lock any computer or console before walking away and will not allow another user to access that computer or console while I am logged on to it.

l. I will not misrepresent, obscure, suppress, or replace a user's identity on the Internet or any VA electronic communication system.

m. I will not auto-forward e-mail messages to addresses outside the VA network.

n. I will comply with any directions from my supervisors, VA system administrators and information security officers concerning my access to, and use of, VA information and information systems or matters covered by these Rules.

o. I will ensure that any devices that I use to transmit, access, and store VA sensitive information outside of a VA protected environment will use FIPS 140-2 approved encryption (the translation of data into a form that is unintelligible without a deciphering mechanism). This includes laptops, thumb drives, and other removable storage devices and storage media (CDs, DVDs, etc.).

p. I will obtain the approval of appropriate management officials before releasing VA information for public dissemination.,

q. I will not host, set up, administer, or operate any type of Internet server on any VA network or attempt to connect any personal equipment to a VA network unless explicitly authorized in writing by my local CIO and I will ensure that all such activity is in compliance with Federal and VA policies.

r. I will not attempt to probe computer systems to exploit system controls or access VA sensitive data for any reason other than in the performance of official duties. Authorized penetration testing must be approved in writing by the VA CIO.

s. I will protect Government property from theft, loss, destruction, or misuse. I will follow VA policies and procedures for handling Federal Government IT equipment and will sign for items provided to me for my exclusive use and return them when no longer required for VA activities.

t. I will only use virus protection software, anti-spyware, and firewall/intrusion detection software authorized by the VA on VA equipment or on computer systems that are connected to any VA network.

u. If authorized, by waiver, to use my own personal equipment, I must use VA approved virus protection software, anti-spyware, and firewall/intrusion detection software and ensure VA the software is configured to meet VA configuration requirements. My local CIO will confirm that the system meets VA configuration requirements prior to connection to VA's network.

v. I will never swap or surrender VA hard drives or other storage devices to anyone other than an authorized OI&T employee at the time of system problems.

w. I will not disable or degrade software programs used by the VA that install security software updates to VA computer equipment, to computer equipment used to connect to VA information systems, or to create, store or use VA information.

x. I agree to allow examination by authorized OI&T personnel of any personal IT device [Other Equipment (OE)] that I have been granted permission to use, whether remotely or in any setting to access VA information or information systems or to create, store or use VA information.

y. I agree to have all equipment scanned by the appropriate facility IT Operations Service prior to connecting to the VA network if the equipment has not been connected to the VA network for a period of more than three weeks.

z. I will complete mandatory periodic security and privacy awareness training within designated timeframes, and complete any additional required training for the particular systems to which I require access.

aa. I understand that if I must sign a non-VA entity's Rules of Behavior to obtain access to information or information systems controlled by that non-VA entity, I still must comply with my responsibilities under the VA National Rules of Behavior when accessing or using VA information or information systems. However, those Rules of Behavior apply to my access to or use of the non-VA entity's information and information systems as a VA user.

bb. I understand that remote access is allowed from other Federal government computers and systems to VA information systems, subject to the terms of VA and the host Federal agency's policies.

cc. I agree that I will directly connect to the VA network whenever possible. If a direct connection to the VA network is not possible, then I will use VA-approved remote access software and services. I must use VA-provided IT equipment for remote access when possible. I may be permitted to use non–VA IT equipment [Other Equipment (OE)] only if a VA-CIO-approved waiver has been issued and the equipment is configured to follow all VA security policies and requirements. I agree that VA OI&T officials may examine such devices, including an OE device operating under an approved waiver, at any time for proper configuration and unauthorized storage of VA sensitive information.

dd. I agree that I will not have both a VA network connection and any kind of non-VA network connection (including a modem or phone line or wireless network card, etc.) physically connected to any computer at the same time unless the dual connection is explicitly authorized in writing by my local CIO.

ee. I agree that I will not allow VA sensitive information to reside on non-VA systems or devices unless specifically designated and approved in advance by the appropriate VA official (supervisor), and a waiver has been issued by the VA's CIO. I agree that I will not access, transmit or store remotely any VA sensitive information that is not encrypted using VA approved encryption.

ff. I will obtain my VA supervisor's authorization, in writing, prior to transporting, transmitting, accessing, and using VA sensitive information outside of VA's protected environment..

gg. I will ensure that VA sensitive information, in any format, and devices, systems and/or software that contain such information or that I use to access VA sensitive information or information systems are adequately secured in remote locations, e.g., at home and during travel, and agree to periodic VA inspections of the devices, systems or software from which I conduct access from remote locations. I agree that if I work from a remote location pursuant to an approved telework agreement with VA sensitive information that authorized OI&T personnel may periodically inspect the remote location for compliance with required security requirements.

hh. I will protect sensitive information from unauthorized disclosure, use, modification, or destruction, including using encryption products approved and provided by the VA to protect sensitive data.

ii. I will not store or transport any VA sensitive information on any portable storage media or device unless it is encrypted using VA approved encryption.

jj. I will use VA-provided encryption to encrypt any e-mail, including attachments to the e-mail, that contains VA sensitive information before sending the e-mail. I will not send any e-mail that contains VA sensitive information in an unencrypted form. VA sensitive information includes personally identifiable information and protected health information.

kk. I may be required to acknowledge or sign additional specific or unique rules of behavior in order to access or use specific VA systems. I understand that those specific rules of behavior may include, but are not limited to, restrictions or prohibitions on limited personal use, special requirements for access or use of the data in that system, special requirements for the devices used to access that specific system, or special restrictions on interconnections between that system and other IT resources or systems.

3. Acknowledgement and Acceptance

a. I acknowledge that I have received a copy of these Rules of Behavior.

b. I understand, accept and agree to comply with all terms and conditions of these Rules of Behavior.

_____ _____

[Print or type your full name] Signature

_____

Date

_____ _____

Office Phone Position Title

DEPARTMENT OF VETERANS AFFAIRS
VETERANS HEALTH ADMINISTRATION
VISN 7- SOUTHEAST NETWORK

Memorandum 10N7- 155
August 28, 2006

PUBLIC KEY INFRASTRUCTURE AND TRANSMISSION OF SENSITIVE DATA

1. **PURPOSE:** This interim guidance provides VISN 7 facilities with approved methods for transmitting sensitive veteran and employee data across Department of Veterans Affairs (VA) networks in the absence of a Department-wide end-to-end encryption capability. The information assets requiring protection comprise all VA sensitive information including veteran protected health information and employee data in messages and transactions in transit through VA or external communication networks.

2. **POLICY:** VA Office of Inspector General (OIG) penetration studies have demonstrated the capability to exploit VA networks, consistently revealing system and administrative passwords and protected health information passed in the clear, and the ability to penetrate VA systems from the Internet. The conclusion of the analysis of several VA-sponsored penetration studies is that the VA network cannot be considered secure. The confidentiality, integrity, or availability of this information is at risk and could be compromised. In the absence of a comprehensive Department-wide solution, to ensure that the provision of health care delivery is foremost and that unnecessary delays are not introduced for the benefit of privacy protections, where risk of harm or injury to the VHA veteran population is threatened, independent judgment needs to be exercised.

3. **DEFINITIONS:**

a. Sensitive information: Sensitive or confidential information is defined as any information the loss of, misuse of, or unauthorized access to, or modification of, could adversely affect the privacy to which individuals are entitled. Sensitive information can be comprised of, but not limited to, the following categories:

1) Information subject to the Privacy Act of 1974
2) Information exempt from the Freedom of Information Act (FOIA)
3) Investigative data
4) Proprietary data, to include selected budgetary data, procurement bids, or information subject to the Tax Reform Act of 1976,
5) Information used by automated decision-making systems that have a high potential for financial loss
6) Information critical to the facility's secure operation
7) Information subject to the HIPAA Security Rule enacted to ensure the confidentiality of electronic protected health information
8) Other information which, if released, might cause harm to any person, adversely affect a Federal program, or whose release is prohibited by law or regulation.

Memorandum 10N7-155
August 28, 2006

4. **PROCEDURES**: To maintain security, VHA employees need to avoid sending sensitive information in unprotected emails and documents across VA networks. When transmission of sensitive data across the VA network is required to meet VA's mission, the following methods should be considered:

a. **Outlook and Exchange Email:**

1) **Public Key Infrastructure (PKI).** The VA PKI provides strong authentication, confidentiality, integrity, and non-repudiation, and is a critical Department-wide system security solution. Departmental information systems that can be protected by VA PKI include Outlook and Exchange electronic mail, Intranet web applications, and remote access services.

a) VA PKI certificates can also be issued to external business partners to protect the transmission of sensitive data. The URL for the VA PKI web site is: http://www.va.gov/proj/vapki/default.htm A list of Local Registration Authorities (LRAs) is posted on the VA PKI web site so that users across the country know who they can contact for guidance on identification (ID) proofing, and issuance of user Personal Identification Numbers (PINs). The official list can be seen at URL http://vaww1.va.gov/proj/vapki/regauth.htm. In addition, a VA Help Desk mail group named 'VA PKI Help' has been established and provides a mechanism for seeking assistance with PKI certificates from VA's PKI support staff.

b) An alternative to issuing individual VA PKI certificates, that provide assurance that sensitive data is not being sent across the VA network via Outlook and/or Exchange email without proper encryption, is to establish designated VA PKI users (subject matter experts) within each facility and have them serve as couriers for transmission of sensitive data. Those designated as the facility Points of Contact (POCs) need to be provided detailed training on requesting, registering, utilizing, and managing their VA PKI certificates, as well as proper procedures for downloading and issuing certificates to individual users.

c) Senders and recipients of electronic mail that contain sensitive information will request to enroll for a PKI certificate from the Local Registration Authority (LRA). The LRAs for VISN 7 are currently the facility ISOs and the OCIS Information Security Officer, Liaison to VA Southeast Network:

i. The request will originate from the user's supervisor or the local ISO and will contain the applicant's name, title, VA Internet address and duty station.

ii. Certificates will expire annually; the VA Digital ID Center will notify the user prior to the expiration date that their certificate is due for renewal.

iii. Users are required to renew their certificate prior to expiration or the enrollment process must be initiated for a new certificate.

iv. Users can enroll and or renew their PKI certificates at the VA Digital ID Center at http://vaww.va.gov/vapki2/. External business partners can enroll and/or renew their certificates at https://www.va.gov/vapkipartners/.

v. When an employee leaves VA or federal service, the facility is required to notify the LRA who will revoke the PKI certificates associated with that employee.

2) **Password-protected Word Documents.** Federal Information Processing Standards (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules, sets forth mandatory provisions for protecting sensitive but unclassified information within computer and telecommunication systems. Effective February 9, 2006, the interim position from the Office of Cyber and Information Security is that they will not support the use of password-protected documents via Microsoft software applications because this approach is not FIPS 140-2 compliant.

b. **Veterans Health Information and Technology Architecture (VistA) Email:** In communicating confidential patient information across local VistA email (within the facility), it is considered appropriate to alert the recipient that there is information in the Computerized Patient Record System (CPRS) from a particular day or visit and that the recipient needs to review. To be secure, the subject line of email never includes a patient's full name or social security number (SSN); the only exception is those emails automatically generated by the VistA system. The subject line; however, may include the first initial of the patient's last name and the last four digits of the SSN (e.g., B.XXXX, not Adam Baker, SSN 123-45-6789). The body of the email message may contain complete patient identifying information. Local VistA email exchanges containing patient health information can become part of the health record if

specifically designated by the practitioner. ***NOTE:*** *This guidance does not apply to email communications that are sent outside of the local VistA system.*

1) **Auto-forwarding of Email.** The VA Chief Information Officer (CIO), in a VA Memorandum dated May 24, 2004, directed that:

   a) Auto-forwarding of email messages to addresses outside the VA network is strictly prohibited.

   b) Facilities are to audit or monitor email traffic to verify compliance with this requirement.

2) **Telephone and Fax.** While outside of the purview of secure transmission of sensitive data across the VA network, alternatives to electronic transmissions include communicating the data via the telephone and/or fax transmissions. Sensitive information should not be transmitted via open network communication channels, including online video conferencing unless such a conference is held on a restricted network.

5. **RESPONSIBILITY**:

a. The Medical Center Director is responsible for safeguarding transmissions of sensitive information using automated information system assets under his/her management control.

b. The LRA is responsible for:
   1) assigning PINs for PKI enrollment to the requestors within ten (10) working days of the request.
   2) maintaining a contact list of PKI applicants.
   3) securely and confidentially distributing the PIN for the applicant to the local ISO.
   4) mailing the PIN to the applicant's supervisor for distribution to the applicant to locations remote to the VAMC.

c. The local ISO is responsible for:
   1) confirming the identity of VA PKI applicants.
   2) arranging delivery of the PIN to the applicant.
   3) revoking the certificates when a user's certificate is subject to revocation.

d. Local IT staff are responsible for assisting in installing the certificate when the user has insufficient system rights to perform the installation, or when technical assistance is required.

e. The PKI user is responsible for:
   1) initiating the request for PKI certificates.

2) the adequate physical protection of the certificate.

3) the timely reporting of compromise or loss of control of the certificate to the LRA that enrolled the user in VA PKI.
4) Installing the certificate on remote computers that transmit sensitive data via Microsoft Outlook because the certificates are both user-specific and machine-specific.
5) Ensuring that sensitive information being transmitted via Microsoft Outlook is being encrypted by PKI.

6. **REFERENCES:**
   a. VA Directive 6213, VA Public Key Infrastructure (VAPKI)
   b. VA Directive 6210, Automated Information Systems Security
   c. Health Information Portability and Accountability Act (HIPAA), 1996
   d. VHA Handbook 1605.1, Privacy and Release of Information

7. **RESCISSIONS:** None.

8. **RECERTIFICATION:** This policy memorandum will be recertified on or before September 2008.

for Thomas A. Cappello, FACHE
Acting Network Director, VA Southeast Network, VISN 7